Verslag internetconsultatie Besluit beveiligde verbinding overheidswebsites en –webapplicaties

Inleiding

Met dit besluit wordt de toepassing van de informatieveiligheidsstandaarden HTTPS en HSTS verplicht voorgeschreven voor publiek toegankelijke websites[1] van bestuursorganen. Het besluit heeft tot doel de beveiliging van deze websites te bevorderen. Gebruikers van overheidswebsites moeten erop kunnen vertrouwen dat informatie-uitwisseling vertrouwelijk verloopt doordat de verbinding met de website beveiligd is, dat de informatie van de website daadwerkelijk afkomstig is van de beheerder van de website en dat de website daadwerkelijk hoort bij de gebruikte domeinnaam. Het besluit verwijst naar de ICT-beveiligingsrichtlijnen van het Nationaal Cyber Security Centrum (NCSC) voor een veilige configuratie van de standaarden. Ook voor dit verslag is een beroep gedaan op expertise van het NCSC.

Internetconsultatie

De formele internetconsultatie stond open van 2 september 2019 tot en met 20 oktober 2019. In totaal zijn 13 reacties binnengekomen. Daarvan zijn 11 reacties openbaar. De reacties zijn afkomstig van overheden (de Provincie Fryslân en de Dienst Publiek en Communicatie van het ministerie van AZ) en private organisaties (Open State Foundation, IIA Nederland, secubeter.nl, FYN Software en RedOps). Daarnaast hebben zes personen een reactie ingebracht.

De noodzaak van het verplicht stellen van de standaarden HTTPS en HSTS wordt door nagenoeg alle respondenten onderschreven. Ook wordt het functionele toepassingsbereik van de verplichting breed onderschreven en is er voldoende draagvlaak om de verplichting toe te passen op zogeheten a-bestuursorganen.

Verschillende reacties bevatten ook voorstellen om bijvoorbeeld andere open standaarden of aanvullende beveiligingsmaatregelen verplicht voor te schrijven. In het onderstaande wordt nader ingegaan op de meest voorkomende voorstellen, voor zover deze niet al zijn afgedekt door de in het besluit genoemde ICT-beveiligingsrichtlijnen van het NCSC. Het gaat achtereenvolgens om 'HSTS-preloading', minimale HSTS-geldigheidsduur, dynamische verwijzing naar ICT-richtlijnen van NCSC, PKIoverheid-certificaten en andere open standaarden.

'HSTS-preloading'

In meerdere reacties wordt gesuggereerd 'HSTS-preloading' op te nemen in het besluit. 'HSTS-preloading' zorgt ervoor dat een website altijd, ook de eerste keer, wordt bezocht via HTTPS. Ondanks dat toepassing van 'HSTS-preloading' in bepaalde gevallen interessant kan zijn, is het naar mening van de regering niet wenselijk om tot

[1] Omwille van de leesbaarheid wordt in dit verslag alleen het begrip 'websites' gebruikt. Dit dient gelezen te worden als 'websites en webapplicaties'.

verplichting hiervan over te gaan. Bestuursorganen moeten hierover van geval tot geval een eigen (risico)afweging kunnen maken. Het NCSC heeft op dit moment geen publicatie die 'HSTS-preloading' beschrijft en is ook niet voornemens om hier een publicatie of nieuwsbericht aan te wijden. Ook maakt 'HSTS-preloading' nu geen onderdeel uit van de opname van HSTS op de 'pas toe of leg uit'-lijst van Forum Standaardisatie.

'HSTS-preloading' is vooral interessant voor de meest gevoelige websites. Websites die HSTS toepassen met een voldoende lange HSTS-geldigheidsperiode (zie ook de paragraaf Minimale HSTS-geldigheidsduur hieronder) dekken de bulk van het risico al af. 'HSTS-preloading' dicht ook het (kleine) restrisico af.

Beheerders die 'HSTS-preloading' voor een bepaald domein willen inschakelen, moeten dit uiterst bedachtzaam doen. Het kan gevolgen hebben voor de toegankelijkheid van bepaalde (sub)domeinen en is niet snel terug te draaien.

Minimale HSTS-geldigheidsduur

Enkele reacties bevatten een aanbeveling voor de HSTS-geldigheidsperiode ('max-age') van websites. Deze periode die de websitebeheerder instelt, bepaalt tot hoe lang na het laatste websitebezoek de browser van de gebruiker bij een opvolgend bezoek direct via HTTPS de website zal verbinden.

In één reactie wordt aanbevolen om de 'HSTS max-age'-instelling op minimaal 1 jaar te zetten. In een andere reactie wordt gepleit voor een geldigheidsperiode van ruim 1 jaar.

De regering acht een HSTS-geldigheidsduur van tenminste twaalf maanden (max-age=31536000) voldoende veilig. Bestuursorganen kunnen zelf de afweging maken om al dan niet een langere geldigheidsduur te hanteren. Bij implementatie is het raadzaam om de geldigheidsduur stapsgewijs te verhogen.

Volgens het NCSC is een levensduur van zes maanden tot een jaar gebruikelijk.[2] Een langere geldigheidsduur heeft als voordeel dat ook infrequentere bezoekers beschermd zijn.

Dynamische verwijzing naar ICT-richtlijnen van NCSC

Meerdere reacties hebben betrekking op de statische verwijzing naar een bepaalde versie van de beveiligingsstandaarden en de ICT-beveiligingsrichtlijnen van het NCSC. Het besluit verwijst naar de ICT-beveiligingsrichtlijnen van het NCSC voor een veilige configuratie van de standaarden. Door ontwikkelingen in de stand van de techniek kunnen bepaalde beveiligingsmaatregelen van de een op de andere dag onvoldoende worden geacht. Bestuursorganen moeten dan snel handelen. Ook zullen de richtlijnen daaraan worden aangepast. Het is volgens de geconsulteerden onwenselijk dat het

[2] https://www.ncsc.nl/documenten/factsheets/2019/juni/01/factsheet-https-kan-een-stuk-veiliger

langere tijd duurt voordat dit besluit is aangepast. Zij stellen daarom een dynamische verwijzing naar de ICT-beveiligingsrichtlijnen van het NCSC voor dan wel een meer abstracte, en daarom duurzame, verplichting om beveiligingsmaatregelen te treffen.

De regering heeft een dynamische verwijzing naar de ICT-beveiligingsrichtlijnen van het NCSC nadrukkelijk overwogen en heeft geconstateerd dat een dynamische verwijzing juridisch niet mogelijk is, en ook niet noodzakelijk is.

Artikel 3 van de voorgenomen Wet digitale overheid (WDO) schrijft voor dat de standaarden worden aangewezen bij algemene maatregel van bestuur. De wetgever heeft het niet mogelijk gemaakt om de aanwijzing daarvan door te delegeren aan de minister. Een dynamische verwijzing in de algemene maatregelen van bestuur naar de ICT-beveiligingsrichtlijnen van het NCSC zou materieel neerkomen op subdelegatie aan de Minister van Justitie en Veiligheid. De minister zou dan de facto voorschrijven welke beveiligingsmaatregelen bestuursorganen moeten toepassen.

Een dynamische verwijzing naar de ICT-beveiligingsrichtlijnen van het NCSC is hier bovendien niet noodzakelijk. Dit besluit schrijft namelijk een minimumnorm voor en belet bestuursorganen niet om meer en verdergaande beveiligingsmaatregelen te treffen. Evenmin doet dit besluit af aan andere wettelijke en beleidsmatige verplichtingen om bepaalde beveiligingsmaatregelen toe te passen. Bestuursorganen kunnen en moeten inspelen op actuele ontwikkelingen. Het is raadzaam om daarvoor de actuele adviezen van het NCSC in de gaten te houden.

Een meer abstracte normstelling zou afdoen aan de concrete meerwaarde van dit besluit. Uit hoofde van verschillende wettelijke en beleidsmatige kaders, waaronder de Algemene verordening gegevensbescherming (AVG) en de Baseline Informatiebeveiliging Overheid (BIO)[3], geldt namelijk reeds een meer algemene verplichting voor bestuursorganen om, rekening houdende met de stand van de techniek, passende beveiligingsmaatregelen te treffen.

Overigens leert de ervaring dat de ICT-beveiligingsrichtlijnen van het NCSC relatief stabiel zijn. De eerste versie van de TLS-richtlijn is vijf jaar van kracht geweest en de huidige versie van de Webapplicatie-richtlijn stamt uit 2015, die daarvoor uit 2012. Onlangs is de TLS-richtlijn geactualiseerd, dit besluit verwijst daarnaar.[4] In geval van wijziging van de ICT-beveiligingsrichtlijnen van het NCSC zal er een proces tot aanpassing van het onderhavige besluit in gang worden gezet.

PKIoverheid-certificaten

Een reactie bevat het voorstel om als eis op te nemen dat overheidsorganisaties PKIoverheid-certificaten moeten gebruiken. Naar mening van de regering valt het buiten de scope van dit besluit om het gebruik van bepaalde certificaten voor te schrijven. Waar nodig, is dit elders al voldoende geborgd. Op grond van de BIO dienen

[3] https://zoek.officielebekendmakingen.nl/stcrt-2019-26526.html

[4] [4] https://www.ncsc.nl/documenten/publicaties/2021/januari/19/ict-beveiligingsrichtlijnen-voor-transport-layer-security-2.1

overheidsorganisaties bijvoorbeeld gebruik te maken van PKIoverheid-certificaten bij web- en mailverkeer van gevoelige gegevens.[5] Sommige generieke voorzieningen vereisen ook dat partijen die aansluiten PKIoverheid-certificaten gebruiken. Zo dienen organisaties die aansluiten op DigiD gebruik te maken van PKIoverheid-certificaten.[6]

Andere open standaarden

Verschillende respondenten stellen voor om ook andere open standaarden, zoals DNSSEC, IPv6, CAA, NEN 7510 en ISO 27001, verplicht voor te schrijven. DNSSEC ('Domain Name System Security Extensions'), een standaard voor domeinnaambeveiliging, wordt het meest genoemd.

Met uitzondering van NEN 7510 en CAA, staan de genoemde standaarden op de pas-toe-of-leg-uit-lijst van Forum Standaardisatie.[7] CAA is hiervoor aangemeld. Voor DNSSEC en IPv6 is ook reeds een zogenaamde streefbeeldafspraak met uiterste implementatiedatum gemaakt.[8][9]

Nadat het besluit voor verplichte toepassing van de informatieveiligheidsstandaarden HTTPS en HSTS in werking is getreden, zal de regering zich beraden voor welke standaard(en) het opportuun is om ook een besluit tot verplichte toepassing te nemen. De in deze consultatie ontvangen reacties op dit punt zullen hierbij worden meegenomen.

[5] https://zoek.officielebekendmakingen.nl/stcrt-2019-26526.html
[6] https://www.logius.nl/diensten/digid/documentatie
[7] https://www.forumstandaardisatie.nl/open-standaarden
[8] https://www.forumstandaardisatie.nl/thema/meting-informatieveiligheidstandaarden-en-adoptieafspraken
[9] https://www.forumstandaardisatie.nl/nieuws/overheid-eind-2021-bereikbaar-ipv6